LABVANTAGE® & 21 CFR PART 11

UNDERSTANDING THE REGULATION AND HOW LABVANTAGE SUCCESSFULLY HELPS CUSTOMERS SUPPORT ITS REQUIREMENTS

LABVANTAGE®
Laboratory Knowledge. Delivered.

EXECUTIVE SUMMARY

The purpose of this paper is to discuss the requirements of 21 CFR Part 11 and provide information on how LABVANTAGE supports the regulation.

Regulatory agencies have given industry guidelines for demonstrating data security and integrity but none address the issue to the same extent as Title 21 Part 11 of the Code of Federal Regulations (Part 11) from the US Food and Drug Administration (FDA). The predicate rule was enacted in March 1997, and it became effective on 20 August 1997. The FDA applied the full force of the law when developing the rule and removed the ambiguity of providing a "guideline" so that electronic records and signatures are ensured to be as trustworthy and reliable as paper records or handwritten signatures. The rule applies to any record, electronic or hand written, or its associated signature, electronic or hand written, that is submitted to the agency (specifically 21 CFR Parts 71, 170, 180, 312, 314, 358, 514, 515, 571, 601, 860, 861, 1003, 1010).

The following paper discusses LABVANTAGE's position in specifically addressing Part 11 requirements for compliance. LabVantage is committed to helping our customers achieve compliance with these regulations.

KEY LABVANTAGE CAPABILITIES ADDRESSING PART 11

In order to begin the discussion of compliance with Part 11, there is some basic information about LABVANTAGE functionality and some assumptions about the deployment and use of LABVANTAGE in a customer setting, which must be understood.

- LABVANTAGE can be deployed as a "closed system" or an "open system with appropriate controls".
- The user name/password security combination in LABVANTAGE is one form of electronic signature. To the extent that current LABVANTAGE records are marked with the current user identification, they satisfy a portion of the requirements for electronic signatures.
- User name/password combinations are given only to one individual.
- The "printed name" referred to in Part 11 is contained in a LABVANTAGE master user record which defines a given system user.
- The user identification captured in LABVANTAGE record stamping is the link to an electronic signature. The user ID and time/date portions of the record stamp are also part of the signature.
- LabVantage can use any electronic signature technology available, for example, biometric identification.
- A "controlled period of access" is the time a person is logged on to LABVANTAGE.
- Passwords are invisible on all displays, and encrypted in the database.
- The "first signing" (using an electronic signature; 11.200 a.1.i) for a user will constitute the logon process.
- Records are unavailable for alteration via other means - outside the use of the system. Since a wide variety of other data maintenance tools exist outside of the system, the client must provide the physical and/or electronic security to avoid the use of the these tools for altering data.
- All records gathered during the use of LABVANTAGE are accurate and complete, since lab personnel actively enter, review, and accept the information contained therein.
- The LABVANTAGE role construct governs access to system functionality. The concept of "meanings" of electronic signings within the regulation is satisfied by a combination of the user's role, e.g. "Approver"; the LABVANTAGE page application e.g., "modify sample"; and the comment entered during the electronic signature process.
- All records are available in human readable form by use of either a reporting engine like Business Objects, InfoMaker, Crystal Reports, etc. or via a helper application like Word, Excel, Notepad, and the like.
- The current system design and development enforces steps and events properly.

SPECIFIC CAPABILITIES TO SUPPORT COMPLIANCE WITH PART 11

The LabVantage Testing and Quality Assurance Departments have built a complete traceability matrix linking the LABVANTAGE requirements to test cases that exercise the Part 11 requirements. LABVANTAGE addresses the software-liable/software enforceable sections of Part 11 and security. Please see the referenced predicate rule for details. In order to comply with this regulation - specific regulatory sections cited are noted in parentheses - LabVantage has done the following in LABVANTAGE:

- Identifying information for an individual is captured in the master user identification table, including the printed name, password and other identifying information (11.50, 11.100.a, 11.200.a.1). This table allows an electronic signature to be disabled by removing the user. Passwords are required.
- The uniqueness of each combination of user ID and password is ensured (11.100.a).
- Each individual's electronic signatures are ensured as unique (11.100.a).
- The ability for many-to-many links between system devices and users has been provided, with an internal integrity checking capability to verify that users have the appropriate authority to access a specific system device. (11.10.h).
- At connection/login each device is verified as acceptable for system input (11.10h).
- Verification that each individual is allowed to use the computer device/workstation from which he/she is logging onto the system is performed (11.10.g, 11.10.h).
- Verification that an individual is allowed to perform a given system function is performed (11.10.g).
- Failed access to the system is logged. All log entries include time/date, user ID, device ID, meaning of action, and success/failure (11.10.d).
- User password encryption is incorporated to allow passwords to be used only by the genuine owner (11.30.2).
- Electronic signatures are captured at "save" points (11.200a.1.i), and links to the signature in all database records are recorded. This is satisfied by the current "user" component of record stamping in LABVANTAGE.
- The use of electronic signatures has been logged as part of the transactional safeguards to prevent unauthorized use (11.300.d).
- Each electronic record is marked with the user ID, time/date, and the "meaning" of the action which created/deleted/modified the record (11.50.b, 11.50.a.2, 11.50.a.3).
- Oracle or Microsoft SQL Server archiving processes have been verified to protect records during records retention processes and enable accurate retrieval of information (11.10c).
- Computer-generated audit trails have been employed for all tables. They are secure, computer generated, time-stamped audit trails for creation/deletion/modification of electronic records (11.10.e).
- Computer-generated audit trails allows for configuring in a reason for change. The reason for change can be made to be a "pull down" menu or free form text entry.
- The reason for change can be configured to be enforced at the time of data commitment or optional depending on the need.
- Electronic signatures have been linked to electronic records (11.70).
- A password aging process that requires users to change their passwords at a regular interval has been incorporated (11.300.b).
- Sequential processing is enforced through workflows (11.10.f).
- The LABVANTAGE master user table disallows record duplication (11.300.a).
- Disallowing users from all roles or changing the user password will "unauthorize" a user's access to LABVANTAGE (11.300.c).
- The standard database allows for both storage of records and retrieval throughout a customer-defined time period (11.10.b).
- The system can be configured to track training records (11.10.i).

REFERENCES: 21 CFR Part 11, Electronic Records Electronic Signatures; [Docket No. 92N-0251]; RIN 0910-AA29; Food and Drug Administration, HHS Final rule: Federal Register 20 March 1997

WWW.LABVANTAGE.COM